

Congress of the United States
Washington, DC 20515

August 22, 2019

The Honorable Steven T. Mnuchin
Secretary
U.S. Department of the Treasury
1500 Pennsylvania Avenue, N.W.
Washington, D.C. 20220

Secretary Mnuchin:

We write to request that the Financial Stability Oversight Council (FSOC or the Council) convene a meeting and consider designating the three leading providers of cloud-based storage systems for the financial industry: Amazon Web Services, Microsoft Azure, and Google Cloud—as systemically important financial market utilities (SIFMUs).

Last month’s data breach at Capital One Financial Corporation (Capital One) was the most recent in a string of incidences demonstrating the dangerous breadth of banks’ and financial institutions’ increasing reliance on cloud computing—and the reach of Amazon Web Services in particular. While it has been determined that an error by Capital One enabled the breach, the incident raises new and serious questions about banks’ and financial institutions’ dependence on cloud services for their data needs—and the risks these systems pose to the safety and stability of the financial system.

Title VIII of the Dodd-Frank Act was enacted to promote stability in the financial system, in part by granting the FSOC the ability to conduct enhanced oversight of Financial Market Utilities (FMUs). Per the Federal Reserve: “In cases where, among other things, a failure or a disruption to the functioning of an FMU could create, or increase, the risk of significant liquidity or credit problems spreading among financial institutions or markets and thereby threaten the stability of the U.S. financial system, the FMU may be designated as systemically important.” Title VIII authorizes the Board of Governors of the Federal Reserve to, among other powers, conduct examinations of, take enforcement action against, and prescribe risk management standards for entities designated as systemically important FMUs, or SIFMUs.¹

¹ “Designated Financial Market Utilities: Title VIII of the Dodd-Frank Act,” *Board of Governors of the Federal Reserve System* at: <https://www.federalreserve.gov/paymentsystems/title-viii-dfa.htm>

According to the FSOC, it must consider the following four factors when analyzing the appropriateness of a SIFMU designation: “(1) the aggregate monetary value of transactions processed by the FMU; (2) the aggregate exposure of the FMU to its counterparties; (3) the relationship, interdependencies, or other interactions of the FMU with other FMUs or payment, clearing, or settlement activities; and (4) the effect that the failure of or a disruption to the FMU would have on critical markets, financial institutions, or the broader financial system.”² Though there are operational differences between cloud service providers and the eight existing SIFMUs, cloud services have become an essential element of our modern financial system and should be overseen commensurately.

First, though the cloud service providers at issue may not process monetary transactions directly, their operational stability underpins an increasing share of banks’ central functions. For example, Bank of America Corporation intends to deliver 80 percent of its technological functions on virtual platforms and with public cloud infrastructure “within the next several years.”³ According to its Chief Technology Officer, Microsoft Azure “continues to see strong cloud adoption from the financial services industry, with more than 80 percent of the world’s largest banks and more than 75 percent of the global systemically important financial institutions using Azure.”⁴ HSBC’s Chief Information Officer expressed similar sentiments at Google’s 2017 Next conference: “Apart from having the \$2.4 trillion of assets on the balance sheet, we also have at the core of the company a massive asset in our data, and what’s been happening in the last two to three years is a massive growth in the size of our data assets.” HSBC uses Google Cloud; the volume of data held at the time of the conference was over 100 petabytes—or 100 million gigabytes.⁵

As data becomes increasingly monetized, hackers become more sophisticated, and firms put more data on servers or the cloud, these breaches are getting more severe. There have been over 9,000 data breaches made public since 2005, which have exposed over 11 billion records in the United States alone.⁶ In 2005, 1.4 million credit card numbers and the names on those accounts, held by DSW Shoe Warehouse, were breached—the first time a breach compromised over a million records. In 2017, the Equifax breach exposed the personally identifiable information of 148 million people.⁷ First reported in July of this year, a data breach at Capital One, which relies on Amazon Web Services for its data storage, compromised over 100 million Capital One

² Dodd-Frank Act section 804(a)(2); 12 U.S.C. § 5463(a)(2).

³ Bank of America chooses the Microsoft Cloud to support digital transformation,” *Microsoft News Center* (Oct. 2017) at: <https://news.microsoft.com/2017/10/02/bank-of-america-chooses-the-microsoft-cloud-to-support-digital-transformation/>

⁴ *Id.*

⁵ James Bourne, “Google gets Colgate, Verizon, HSBC on board – a customer step up for enterprise cloud,” *Cloud Tech* (March 2017) at: <https://www.cloudcomputing-news.net/news/2017/mar/13/google-gets-colgate-verizon-hsbc-board-customer-step-enterprise-cloud/>

⁶ “Data Breaches,” *Privacy Rights Clearinghouse* at: <https://www.privacyrights.org/data-breaches>

⁷ Merrit Kennedy, “Equifax Says 2.4 Million More People Were Impacted By Huge 2017 Breach,” *NPR* (March 2018) at: <https://www.npr.org/sections/thetwo-way/2018/03/01/589854759/equifax-says-2-4-million-more-people-were-impacted-by-huge-2017-breach>

customer accounts and credit card applications.⁸ Though cloud service providers may not process monetary transactions like other SIFMUs, these firms provide the world's biggest banks with the technological foundation necessary to link to one another and other financial and commercial market participants, thereby helping to enable monetary and commercial transactions while simultaneously maintaining their clientele's most sensitive information and associated assets.

With regard to the second factor, though there is no direct financial exposure if the cloud fails, the counterparty exposure in the form of a failure to provide the cloud service—and the operational losses that stem from that failure—could be significant.

Third, the volatility of public confidence in cloud services and the necessity of data integrity to maintaining that confidence is common to all cloud service providers. A data breach or other disruptive event that shakes public perception of the trustworthiness of the cloud could discourage consumers from using cloud-reliant banks and potentially spur a bank run. Should any cloud service provider fail, public mistrust of the service would not be limited to that one company. Particularly given the rapid speed of technological development, enforcing appropriate safeguards is critical to maintaining continued public acceptance of the cloud.

Fourth, the effect of a disruption to a cloud services provider on the broader financial system could be catastrophic. According to a 2016 report by McKinsey, 100 percent of financial institutions use cloud services in some capacity.⁹ In addition to financial institutions, our government has come to rely on Amazon Web Services for a massive share of its data storage needs: the Department of Defense holds a \$10 billion cloud computing contract with Amazon Web Services, and NASA and the state of Arizona are also clients of AWS.¹⁰ An Amazon Web Services cloud failure in particular would debilitate major swaths of the financial industry, basic government functions, and our national security.

It is important to note that not all four factors are weighted equally. According to the FSOC in its 2011 Rule describing the criteria the Council would consider in designating SIFMUs, “the two critical determinations for an FMU designation are: (1) Whether the failure of or a disruption to the functioning of the FMU now or in the future could create, or increase, the risk of significant liquidity or credit problems spreading among financial institutions or markets (the “First Determination”); and (2) Whether the spread of such liquidity or credit problems among

⁸ Rob McLean, “A hacker gained access to 100 million Capital One credit card applications and accounts,” CNN (July 2019) at: <https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html>

⁹ Nagendra Bommadevara, Andrea Del Miglio, and Steve Jansen, “Cloud Adoption to Accelerate IT Modernization,” *McKinsey Digital* (April 2018) at: <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/cloud-adoption-to-accelerate-it-modernization>

¹⁰ Jefferson Graham, “Capital One data breach: Amazon Web Services is backbone for Netflix, NASA and others,” *USA Today* (July 2019) at: <https://www.usatoday.com/story/tech/talkingtech/2019/07/30/amazon-aws-unit-says-its-not-responsible-capital-one-data-breach/1868862001/>

financial institutions or markets could threaten the stability of the financial system of the United States (the “Second Determination”).”¹¹

While not all banks have made public their cloud service providers, among major financial institutions, Capital One and Liberty Mutual use Amazon Web Services,¹² Bank of America uses Microsoft Azure,¹³ and HSBC uses Google Cloud.¹⁴ Fifty-seven percent of the cloud services market is cornered by those three providers: in the first quarter of this year, Amazon Web Services controlled 33 percent of the market, Microsoft Azure 16 percent, and Google Cloud 8 percent.¹⁵ Given the technical nature of computing services, a firm like Bank of America would not be able to quickly transfer its cloud services to Amazon Web Services, should Microsoft Azure fail. In the interim, while the cloud was nonfunctional, the bank would be unable to perform up to 80 percent of its technological functions—potentially creating significant liquidity disruptions.¹⁶ A lack of substitutability for the services provided by these very few firms creates systemic risk; a disruption at any major cloud computing platform would cause widespread and immediate harm and compromise the stability of the market.

Additionally, cloud services are not currently subject to an appropriate and enforced regulatory regime. In April, Federal Reserve examiners assessed an Amazon.com facility in Virginia,¹⁷ using their limited power under the Bank Service Company Act to oversee nonbank vendors that provide the software to run banks’ deposit and loan platforms.¹⁸ “Chaperoned by an Amazon employee, they were allowed to review certain documents on Amazon laptops, but not allowed to take anything with them.”¹⁹ The perfunctory review of a handful of Amazon-selected documents over the course of a few hours, on-site, is not meaningful oversight. Without a dedicated regulatory regime proportional and tailored to their very unique structure and risks, cloud computing companies will continue to evade supervision.

Our concerns are shared by the world’s major financial market regulators. In February of this year, the Financial Stability Board—an international body comprised of the G-20’s central banks

¹¹ “Authority To Designate Financial Market Utilities as Systemically Important,” Final Rule, Financial Stability Oversight Council, *Federal Register* (July 2011) at <https://www.federalregister.gov/documents/2011/07/27/2011-18948/authority-to-designate-financial-market-utilities-as-systemically-important>

¹² Jefferson Graham, “Capital One data breach: Amazon Web Services is backbone for Netflix, NASA and others,” *USA Today* (July 2019) at: <https://www.usatoday.com/story/tech/talkingtech/2019/07/30/amazon-aws-unit-says-its-not-responsible-capital-one-data-breach/1868862001/>

¹³ “Bank of America chooses the Microsoft Cloud to support digital transformation,” *Microsoft News Center* (Oct. 2017) at: <https://news.microsoft.com/2017/10/02/bank-of-america-chooses-the-microsoft-cloud-to-support-digital-transformation/>

¹⁴ “HSBC To Launch AML System With Google Cloud,” *PYMNTS.com* (Nov. 2018) at: <https://www.pymnts.com/news/security-and-risk/2018/hsbc-anti-money-laundering-google-cloud/>

¹⁵ Nicole Henderson, “Cloud Market Share: AWS Still Ahead, But Watch Google Grow,” *ITPro Today* (May 2019) at: <https://www.itprotoday.com/iaaspaas/cloud-market-share-aws-still-ahead-watch-google-grow>

¹⁶ “Bank of America chooses the Microsoft Cloud to support digital transformation,” *Microsoft News Center* (Oct. 2017) at: <https://news.microsoft.com/2017/10/02/bank-of-america-chooses-the-microsoft-cloud-to-support-digital-transformation/>

¹⁷ Liz Hoffman, Dana Mattioli, and Ryan Tracy, “Fed Examined Amazon’s Cloud in New Scrutiny for Tech,” *Wall Street Journal* (August 2019) at: https://www.wsj.com/articles/fed-examined-amazons-cloud-in-new-scrutiny-for-tech-11564693812?mod=hp_lead_pos6

¹⁸ 12 U.S.C. § 1867

¹⁹ *Id.*

and supervisors—noted that Big Tech is invading the financial sector and could upend the stability of the market.²⁰ In April, top European Union financial regulators issued a report in which they advocated for legislation to monitor cloud computing services that are central to financial institutions. The supervisors highlighted the vulnerabilities implicit in the financial industry’s heavy reliance on third parties and noted that their concerns are “especially acute with regard to cloud services.”²¹

Given the serious and far-reaching risks inherent in our reliance on a handful of cloud service providers to maintain the basic functioning of our economy, we ask that you consider designating as SIFMUs the country’s largest cloud service providers, including but not limited to Amazon Web Services, Google Cloud, and Microsoft Azure. Please respond by September 15th with a description of the FSOC’s plan to consider these designations. If the Council will not evaluate the appropriateness of using its authority under 12 U.S.C. § 5463 to regulate cloud computing providers, please respond with your reasoning.

Sincerely,



Congresswoman Katie Porter



Congresswoman Nydia M. Velázquez

cc: Andrew R. Jassy, Chief Executive Officer, Amazon Web Services
Thomas Kurian, Chief Executive Officer, Google Cloud
Mark Russinovich, Chief Technology Officer, Microsoft Azure

²⁰ Silla Brush, “Big Tech Is Coming for Big Bank Profits, Finance Regulators Warn,” *Bloomberg* (Feb. 2019) at: <https://www.bloomberg.com/news/articles/2019-02-14/big-tech-is-coming-for-big-bank-profits-finance-regulators-warn>

²¹ *Id.*